Quantum Computation
(Lecture 1)

Luís Soares Barbosa

MSc Physics Engineering

Universidade do Minho, 2021-22

Physics of information

$\boxed{\text{Information}}$

is encoded in the state of a physical system

$\boxed{\text{Computation}}$

is carried out on an actual physically realizable device

- the study of information and computation cannot ignore the underlying physical processes.
- ... although progress in Computer Science has been made by abstracting from the physical reality
- more precisely: by building more and more abstract models of a sort of reality, i.e. a way of understanding it
- ... and if this way changes?

A short, long way to go ...

How physics constrains our ability to use and manipulate information?

- Landauer's principle (1961): information deleting is necessarily a dissipative process.
- Charles Bennett (1973): any computation can be performed in a reversible way, and so with no dissipation.

NAND $\Longrightarrow$ Toffoli

$$(x, y) \mapsto \neg(x \wedge y) \qquad (x, y, z) \mapsto (x, y, z \oplus (x \wedge y))$$

with $z = 1$

A short, long way to go ...

Information is physical, and the physical reality is quantum mechanical:

How does quantum theory shed light on the nature of information?

- Quantum dynamics is truly random
- Acquiring information about a physical system disturbs its state (which is related to quantum randomness)
- Noncommuting observables cannot simultaneously have precisely defined values: the uncertainty principle
- Quantum information cannot be copied with perfect fidelity: the no-cloning theorem (Wootters, Zurek, Dieks, 1982)
- Quantum information is encoded in nonlocal correlations between the different parts of a physical system, i.e. the predictions of quantum mechanics cannot be reproduced by any local hidden variable theory (John Bell, 1967)

Quantum computing

The meaning of computable remains the same

A classical computer can simulate a quantum computer to arbitrarily good accuracy.

... but the order of complexity may change

but the simulation is computationally hard, i.e. extremely inefficient as the number of qubits increases:

- For 100 qubits the state space would require to store $2^{100} \approx 10^{30}$ complex numbers!
- And what about rotating a vector in a vector space of dimension 10^{30}?

Quantum computing

In a sense this is not the decisive argument:

Simulating the evolution of a vector in an exponentially large space can be done locally through a probabilistic classical algorithm in which each qubit has a value at each time step, and each quantum gate can act on the qubits in various possible ways, one of which is selected as determined by a (pseudo)-random number generator.

... After all, the computation provides a means of assigning probabilities to all the possible outcomes of the final measurement...

Quantum computing

However, Bell's result precludes such a simulation: there is no local probabilistic algorithm that can reproduce the conclusions of quantum mechanics.

In the presence of entanglement, one can access only an exponentially small amount of information by looking at each subsystem separately.

Quantum computing as using quantum reality as a computational resource

Richard Feynman, *Simulating Physics with Computers* (1982)

How? From a probabilistic machine ...

States: Given a set of possible configurations, states are vectors of probabilities in $\mathcal{R}^n$ which express indeterminacy about the exact physical configuration, e.g. $\left[p_0 \cdots p_n\right]^T$ st $\sum_i p_1 = 1$
Operator: double stochastic matrix (*must come (go) from (to) somewhere*), where $M_{i,j}$ specifies the probability of evolution from configuration j to i
Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current probabilities

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: the system is always in some configuration — if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$

How? From a probabilistic machine ...

Composition:

$$p \otimes q \;=\; \begin{bmatrix} p_1 \\ 1-p_1 \end{bmatrix} \otimes \begin{bmatrix} q_1 \\ 1-q_1 \end{bmatrix} \;=\; \begin{bmatrix} p_1 q_1 \\ p_1(1-q_1) \\ (1-p_1)q_1 \\ (1-p_1)(1-q_1) \end{bmatrix}$$

- correlated states: cannot be expressed as $p \otimes q$, e.g.

$$\begin{bmatrix} 0.5 \\ 0 \\ 0 \\ 0.5 \end{bmatrix}$$

- Operators are also composed by $\otimes$ (Kronecker product):

$$M \otimes N \;=\; \begin{bmatrix} M_{1,1}N & \cdots & M_{1,n}N \\ \vdots & & \vdots \\ M_{m,1}N & \cdots & M_{m,n}N \end{bmatrix}$$

... to a quantum machine

States: given a set of possible configurations, states are unit vectors of (complex) amplitudes in $\mathcal{C}^n$

Operator: unitary matrix ($M^\dagger M = I$). The norm squared of a unitary matrix forms a double stochastic one.

Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current amplitudes (wave function)

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: configuration i is observed with probability $\|\alpha_i\|^2$ if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$

Composition: also by a tensor on the complex vector space; may exist entangled states

The quest for efficient quantum algorithms

$\boxed{\text{Factoring in polynomial time - } \mathcal{O}((\ln n)^3)}$

Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* (1994)

- Classically believed to be superpolynomial in log n, i.e. as n increases the worst case time grows faster than any power of log n.
- The best classical algorithm requires approximately

$$e^{1.9(\sqrt[3]{\ln\ n}\sqrt[3]{(\ln\ \ln\ n)^2})}$$

- From the best current estimation (the 65 digit factors of a 130 digit number can be found in around one month in a massively parallel computer network) one can extrapolate that to factor a 400 digit number will take about the age of the universe (10^{10} years)

The quest for efficient quantum algorithms

The quest

- Non exponential speedup. Not relevant for the complexity debate, but shed light on what a quantum computer can do.
  Example: Grover's search of an unsorted data base.
- Exponential speedup relative to an oracle. By feeding quantum superpositions to an oracle, one can learn what is inside it with an exponential speedup.
  Example: Simon's algorithm for finding the period of a unction.
- Exponential speedup for apparently hard problems
  Example: Shor's factoring algorithm.

The quest for efficient quantum algorithms

The structure of a quantum algorithm

1. State preparation
   (fix initial setting)
2. Transformation
   (combination of unitary transformations)
3. Measurement
   (projection onto a basis vector associated with a measurement tool)

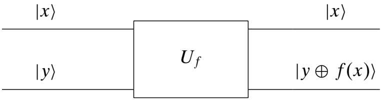
What's next?

1. Study a number of algorithmic techniques
2. and their application to the development of quantum algorithms

The Deutsch problem

$\boxed{\text{Is } f : \mathbf{2} \longrightarrow \mathbf{2} \text{ constant, with a unique evaluation?}}$

Oracle



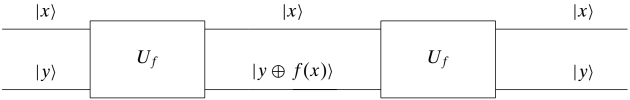
where $\oplus$ stands for exclusive or, i.e. addition module 2.

- The oracle takes input $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$
- Fixing $y = 0$ the output is $|x\rangle|f(x)\rangle$

Is the oracle a **quantum gate**?

First of all, one must prove that

- The oracle is a unitary, i.e. reversible gate



$$|x\rangle|(y \oplus f(x)) \oplus f(x)\rangle \;=\; |x\rangle|y \oplus (f(x) \oplus f(x))\rangle \;=\; |x\rangle|y \oplus 0\rangle \;=\; |x\rangle|y\rangle$$

The Deutsch problem

Preparing the first qubit as $|x\rangle$ is the (quantum version of) input x:

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|f(0)\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle|f(1)\rangle \end{aligned}$$

But in the quantum world, one can better: input a superposition of $|0\rangle$ and $|1\rangle$ to get

$$|\frac{|0\rangle + |1\rangle}{\sqrt{2}}, 0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,|0\rangle \mapsto \cdots$$

The Deutsch problem

...

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2}}|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,|0\rangle\right) &= \frac{1}{\sqrt{2}}U_f|0\rangle|0\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|0\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle|0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f(1)\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle \end{aligned}$$

- The value of f on both possible inputs (0 and 1) was computed simultaneously in superposition
- Double evaluation — the bottleneck in a classical solution — was avoided by superposition

Is such **quantum parallelism** useful?

NO

Although both values have been computed simultaneously, only one of them is retrieved upon measurement in the computational basis: Actually, 0 or 1 will be retrieved with identical probability (why?).

YES

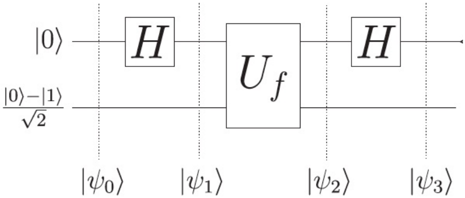
The Deutsch problem is not interested on the concrete values f may take, but on a global property of f: whether it is constant or not, technically on the value of

$$f(0) \oplus f(1)$$

The Deutsch algorithm explores another quantum resource — interference — to obtain that global information on f

Deutsch algorithm

Idea: Avoid double evaluation by superposition and interference



The circuit computes:

$$|\psi_1\rangle = |+\rangle|-\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

Deutsch algorithm

After the oracle, at φ_2, one obtains

$$|x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \Leftarrow f(x) = 0 \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} & \Leftarrow f(x) = 1 \end{cases}$$
$$= (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

For $|x\rangle = |+\rangle$ a superposition:

$$|\psi_2\rangle = \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$
$$= \begin{cases} (\pm 1)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases}$$

Deutsch algorithm

$$
\begin{aligned}
|\psi_3\rangle &= H|\psi_2\rangle \\
&= \begin{cases} (\pm 1)\,|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\,|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases}
\end{aligned}
$$

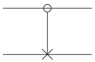
To answer the original problem is now enough to measure the first qubit: if it is in state $|0\rangle$, then f is constant.

Note

As the initial state in the second qubit can be prepared as $H|1\rangle$, the circuit is equivalent to

$$(H \otimes I)\, U_f\, (H \otimes H)(|01\rangle)$$

Recalling the *CNOT* gate



$$\overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{CNOT}$$ corresponds to the oracle: $|xy\rangle \mapsto |x, x \oplus y\rangle$

$$\begin{aligned} CNOT|0\rangle|\varphi\rangle &= |0\rangle I|\varphi\rangle \\ CNOT|1\rangle|\varphi\rangle &= |1\rangle X|\varphi\rangle \end{aligned}$$

Recall its effect when applied in the Hadamard basis, e.g.

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \mapsto \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

The phase jumps, or is kicked back, from the second to the first qubit.

The phase 'kick back' technique

This happens because $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of

- X (with $\lambda = -1$) and of I (with $\lambda = 1$)
- and, thus, $X \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -1 \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ and $I \frac{|0\rangle - |1\rangle}{\sqrt{2}} = 1 \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Thus,

$$\begin{aligned} CNOT\,|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= |1\rangle \left(X \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= |1\rangle \left((-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

while $CNOT\,|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

The phase 'kick back' technique

The phase has been kicked back to the first (control) qubit:

$$CNOT\,|i\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \;=\; (-1)^i|i\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

for $i \in \{0,1\}$, yielding, when the first (control) qubit is in a superposition of $|0\rangle$ and $|1\rangle$,

$$CNOT\,(\alpha|0\rangle+\beta|1\rangle)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \;=\; (\alpha|0\rangle-\beta|1\rangle)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The phase 'kick back' technique

Input an eigenvector to the target qubit of operator $\widehat{U}_{f(x)}$, and associate the eigenvalue with the state of the control qubit

Phase ‘kick back’ in the Deutsch algorithm

Instead of *CNOT*, an oracle U_f for an arbitrary Boolean function $f : \mathbf{2} \longrightarrow \mathbf{2}$, presented as a controlled-gate, i.e. a 1-gate $\widehat{U}_{f(x)}$ acting on the second qubit and controlled by the state $|x\rangle$ of the first one, mapping

$$|y\rangle \;\mapsto\; |y \oplus f(x)\rangle$$

The critical issue is that state $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of $\widehat{U}_{f(x)}$

Phase 'kick back' in the Deutsch algorithm

$$
\begin{aligned}
U_f\,|x\rangle|-\rangle &= |x\rangle \widehat{U}_{f(x)}|-\rangle \\
&= \left(\frac{|x\rangle \widehat{U}_{f(x)}\,|0\rangle - |x\rangle \widehat{U}_{f(x)}\,|1\rangle}{\sqrt{2}}\right) \\
&= \left(\frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\
&= |x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\
&= |x\rangle(-1)^{f(x)} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle(-1)^{f(x)}|-\rangle
\end{aligned}
$$

Thus, when the control qubit is in a superposition of $|0\rangle$ and $|1\rangle$,

$$
U_f\,(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \Big((-1)^{f(0)}\alpha|0\rangle + (-1)^{f(1)}\beta|1\rangle\Big)\,|-\rangle
$$

Generalizing Deutsch ...

Generalizing Deutsch's algorithm to functions whose domain is an

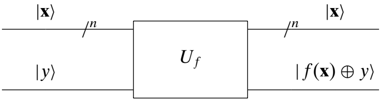
initial segment $N = 2^n$ of $\mathbb{N}$ encoded into a binary string

i.e. the set of natural numbers from 0 to $\mathbf{2}^n - 1$

The Deutsch-Jozsa problem

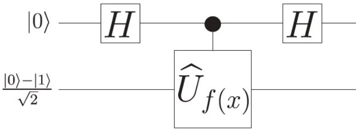
$\boxed{\text{Assuming } f : \mathbf{2}^n \longrightarrow \mathbf{2} \text{ is either balanced or constant, determine which is the case with a unique evaluation}}$

The oracle

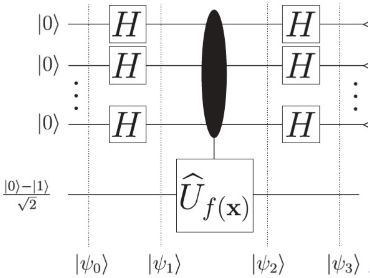


Generalizing Deutsch ...

The Deutsch circuit



The Deutsch-Joza circuit



The Deutsch-Jozsa Algorithm

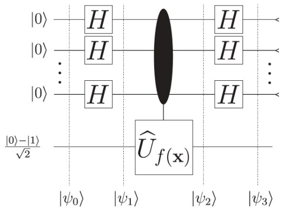
The crucial step is to compute $H^{\otimes n}$ over n qubits:

$$\begin{aligned} H^{\otimes n}|0\rangle^{\otimes n} &= \left(\frac{1}{\sqrt{2}}\right)^n \underbrace{(|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}_{n} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{2}^n} |x\rangle \end{aligned}$$

Thus

$$\begin{aligned} \psi_0 &= |0\rangle^{\otimes n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ \psi_1 &= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{2}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

The Deutsch-Jozsa Algorithm



The phase kick-back effect

$$\psi_2 = \frac{1}{\sqrt{2^n}} U_f \left(\sum_{x \in \mathbf{2}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{2}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

The Deutsch-Jozsa Algorithm

Finally, we have to compute the last stage of $H^{\otimes}$ application.

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x}|1\rangle) = \frac{1}{\sqrt{2}}\sum_{z\in\mathbf{2}}(-1)^{xz}|z\rangle$$

$$\begin{aligned}
H^{\otimes}|x\rangle &= H^{\otimes}(|x_1\rangle, \cdots, |x_n\rangle) \\
&= H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)\,\cdots\,\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_n}|1\rangle) \\
&= \frac{1}{\sqrt{2^n}}\sum_{z_1 z_2 \cdots z_n \in \mathbf{2}}(-1)^{x_1 z_1 + x_2 z_2 + \cdots + x_n z_n}|z_1\rangle|z_2\rangle\cdots|z_n\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{z\in\mathbf{2}^n}(-1)^{x.z}|z\rangle
\end{aligned}$$

The Deutsch-Jozsa Algorithm

$$
\begin{aligned}
|\psi_3\rangle &= \frac{\sum_{x\in\mathbf{2}^n}(-1)^{f(x)}\sum_{z\in 2^n}(-1)^{z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{\sum_{x,z\in\mathbf{2}^n}(-1)^{f(x)}(-1)^{z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{\sum_{x,z\in\mathbf{2}^n}(-1)^{f(x)+z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}}
\end{aligned}
$$

Note that the amplitude for state $|z\rangle = |0\rangle$ is

$$
\frac{1}{2^n}\sum_{x\in\mathbf{2}^n}(-1)^{f(x)}
$$

The Deutsch-Jozsa Algorithm

Analysis

$\boxed{f \text{ is constant at } 1} \quad \rightsquigarrow \quad \frac{-(2^n)|0\rangle}{2^n} = -|0\rangle$

$\boxed{f \text{ is constant at } 0} \quad \rightsquigarrow \quad \frac{(2^n)|0\rangle}{2^n} = |0\rangle$

As $|\varphi_3\rangle$ has unit length, all other amplitudes must be 0 and the top qubits collapse to $|0\rangle$

$\boxed{f \text{ is balanced}} \quad \rightsquigarrow \quad \frac{0|0\rangle}{2^n} = 0|0\rangle$

because half of the x will cancel the other half. The top qubits collapse to some other basis state, as $|0\rangle$ has zero amplitude

$\boxed{\text{The top qubits collapse to } |0\rangle \text{ iff } f \text{ is constant}}$

Quantum Algorithms

The Deutsch-Jozsa algorithm: Lessons learnt

- Exponential speed up: f was evaluated once rather than $2^n - 1$ times
- The quantum state encoded global properties of function f
- ... that can be extracted by exploiting cleverly such non local correlations.

Quantum Algorithms

The remaining of this course will explore

Classes of quantum algorithm

- Based on the quantum Fourier transform: The Deutsch-Jozsa is a simple example; Phase estimation; Shor algorithm; etc.
- Based on amplitude amplification: Variants of Grover algorithm for search processes.
- Quantum simulation.

and come back to complexity in the end.
However a proper algorithmic science is still lacking
(more next year in *Quantum Logic*)